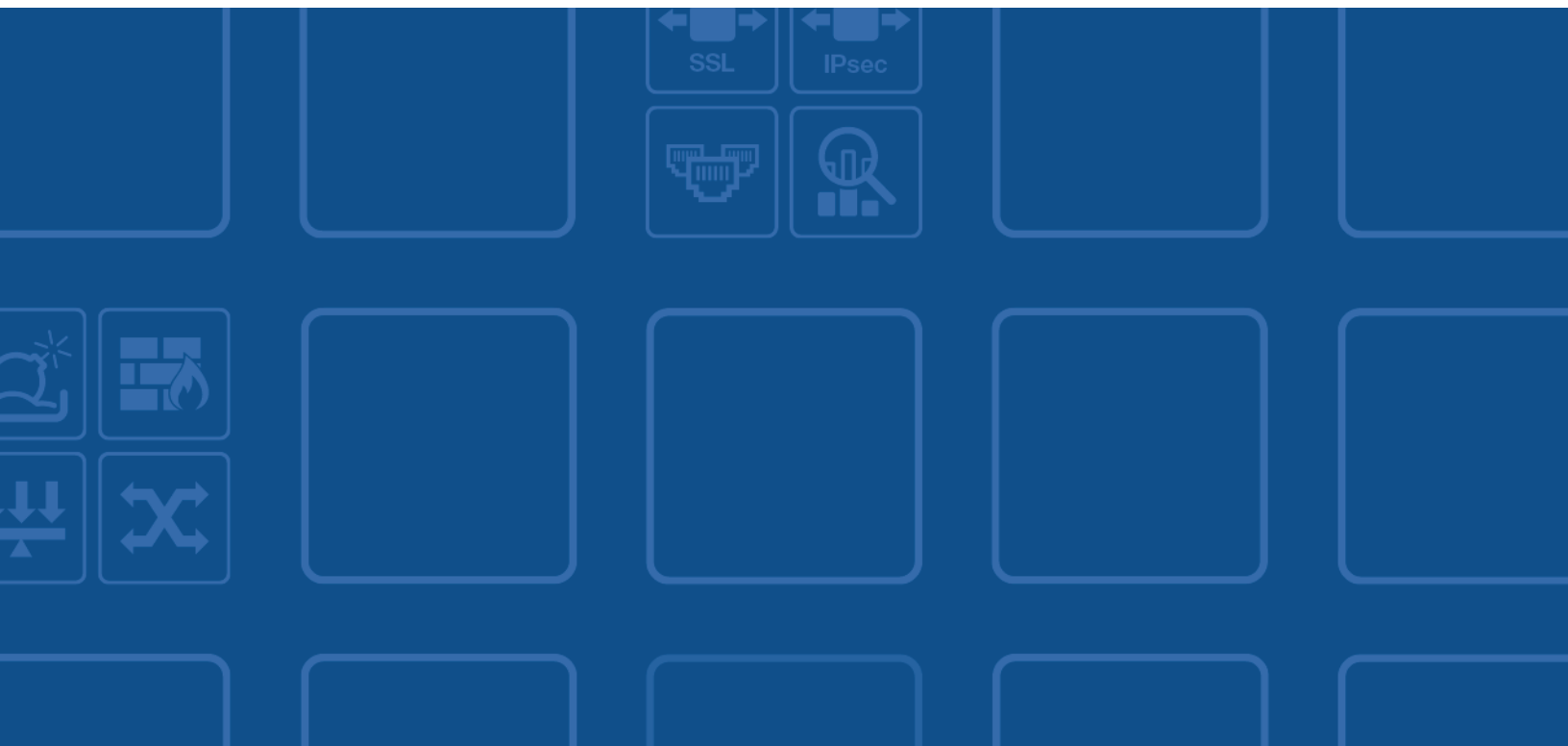
FORTINET
High Performance Network Security

FortiAnalyzer VM - Install Guide

VERSION 5.4



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

April 11, 2017

FortiAnalyzer VM 5.4 Install Guide

05-540-309958-20170411

TABLE OF CONTENTS

Change Log

Date	Change Description
2016-03-17	Initial release.
2016-06-29	Microsoft Azure instructions added. 32bit VM images removed in 5.4.1.
2016-09-06	Updated VM-BASE storage capacity to 500GB.
2016-09-16	AWS default password information updated.
2017-03-28	Minimum system requirements added.
2017-04-11	KVM storage cache mode updated to *writethrough*.

Introduction

The FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine-tune your policies. Organizations of any size will benefit from centralized security event logging, forensic research, reporting, content archiving, data mining and malicious file quarantining.

FortiAnalyzer offers enterprise class features to identify threats, while providing the flexibility to evolve along with your ever-changing network. FortiAnalyzer can generate highly customized reports for your business requirements, while aggregating logs in a hierarchical, tiered logging topology.

This document describes how to deploy a FortiAnalyzer virtual appliance in several virtualization server environments. This includes how to configure the virtual hardware settings of the virtual appliance. This guide presumes that the reader has a thorough understanding of virtualization servers.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For that information, see the *FortiAnalyzer Administration Guide* in the Fortinet Document Library.

FortiAnalyzer documentation

The following FortiAnalyzer product documentation is available:

- *FortiAnalyzer Administration Guide*
  This document describes how to set up the FortiAnalyzer system and use it with supported Fortinet units.
- *FortiAnalyzer device QuickStart Guides*
  These documents are included with your FortiAnalyzer system package. Use these document to install and begin working with the FortiAnalyzer system and GUI.
- *FortiAnalyzer Online Help*
  You can get online help from the FortiAnalyzer GUI. FortiAnalyzer online help contains detailed procedures for using the GUI to configure and manage devices.
- *FortiAnalyzer CLI Reference*
  This document describes how to use the FortiAnalyzer Command Line Interface (CLI) and contains references for all CLI commands.
- *FortiAnalyzer Release Notes*
  This document describes new features and enhancements in the FortiAnalyzer system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.
- *FortiAnalyzer VM Install Guide*
  This document, which describes installing FortiAnalyzer VM in your virtual environment.

License and System Requirements

Licensing

Fortinet offers the FortiAnalyzer VM in a stackable license model. This model allows you to expand your VM solution as your environment expands.For information on purchasing a FortiAnalyzer VM license, contact your Fortinet Authorized Reseller, or visit http://www.fortinet.com/how_to_buy/.

When configuring your FortiAnalyzer VM, ensure to configure hardware settings as outlined in the following table and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

	GB / Day of logs	Storage Capacity
VM-BASE	1	500GB
VM-GB1	+1	+500GB
VM-GB5	+5	+3TB
VM-GB25	+25	+10TB
VM-GB100	+100	+24TB
VM-GB500	+500	+48TB
VM-GB2000	+2000	+100TB

For more information, see Minimum system requirements on page 8, and the FortiAnalyzer product data sheet:

http://www.fortinet.com/sites/default/files/productdatasheets/FortiAnalyzer-VM.pdf.

After placing an order for FortiAnalyzer VM, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiAnalyzer VM with Customer Service & Support at https://support.fortinet.com.

Upon registration, you can download the license file. You will need this file to activate your FortiAnalyzer VM. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded and validated, the CLI and GUI will be fully functional.

Evaluation license

FortiAnalyzer VM includes a free, full featured 15 day trial license. No activation is required for the built-in evaluation license.

The trial period begins the first time you start the FortiAnalyzer VM. When the trial expires, all functionality is disabled until you upload a license file.

Technical support is not included with the 15-day evaluation.

Contact your Fortinet Reseller to request a full evaluation (60-days) license.

Minimum system requirements

The following table lists the minimum system requirements for your VM hardware, based on the number of logs, the log rate, and the number of devices, VDOMs, or ADOMs that your VM manages.

Analytic Sustained Rate (logs/sec)	GB/Day of Logs	Maximum Devices / VDOMs / ADOMs	VM Hardware Requirements		
			RAM (GB)	CPU cores	IOPS
500	75	200	8	2	100
4000	300	2000	16	6	300
7500	500	2000	32	6	600
35000	1600	4000	64	16	1500
48000	4000	10000	64	16	2000
60000	5000	10000	128	24	2500

The collector sustained rate can be calculated by multiplying the analytic sustained rate by 1.5.

This table does not take into account other hardware specifications, such as bus speed, CPU model, or storage type.

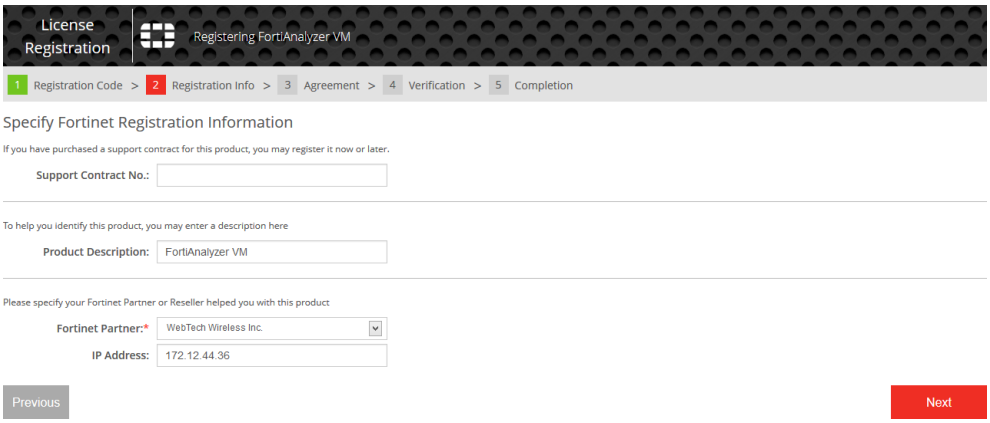
Registration and Deployment

Register with Customer Service & Support

To obtain the FortiAnalyzer VM license file you must first register your FortiAnalyzer VM with Fortinet Customer Service & Support.

To register your FortiAnalyzer VM:

1. Log in to the Fortinet Customer Service & Support portal using an existing support account or click *Create an Account* to create a new account.
2. In the toolbar select *Asset* > *Register/Renew*. The *Registration Wizard* opens.
3. Enter the registration code from the FortiAnalyzer VM License Certificate that was emailed to you, select the end user type, and then click *Next*. The *Registration Info* page is displayed.

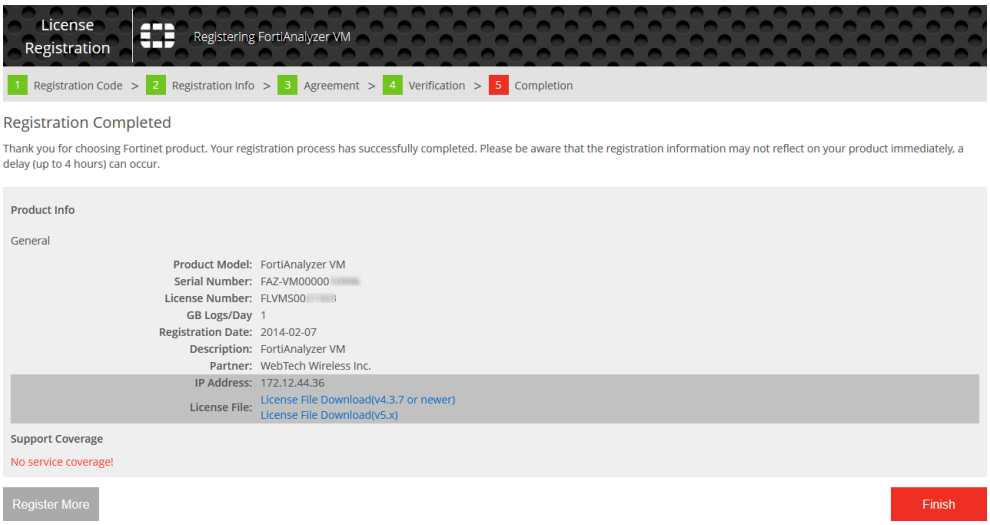


4. Enter your support contract number, product description, Fortinet Partner, and IP address in the requisite fields, then select *Next*.

As a part of the license validation process FortiAnalyzer VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiAnalyzer VM's IP address has been changed, the FortiAnalyzer VM must be rebooted in order for the system to validate the change and operate with a valid license.

The Customer Service & Support portal currently does not support IPv6 for FortiAnalyzer VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

5. On the *Fortinet Product Registration Agreement* page, select the checkbox to indicate that you have read, understood, and accepted the service contract, then select *Next* to continue to the *Verification* page.
6. The verification page displays the product entitlement. Select the checkbox to indicate that you accept the terms then select *Confirm* to submit the request.

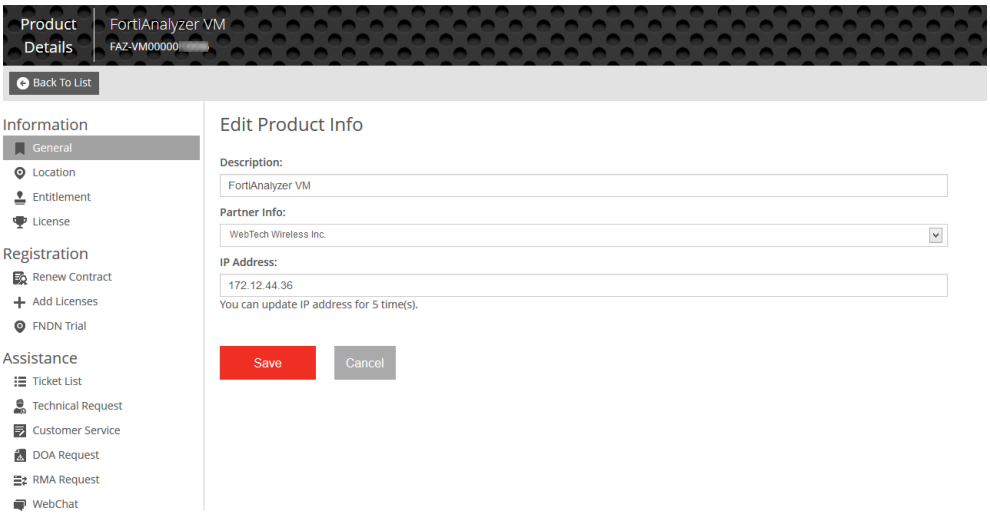


7. From the *Registration Completed* page you can download the FortiAnalyzer VM license file, select *Register More* to register another FortiAnalyzer VM, or select *Finish* to complete the registration process.

   Select *License File Download* to save the license file (`.lic`) to your management computer. See Upload the license file on page 47 for instructions on uploading the license file to your FortiAnalyzer VM via the GUI.

To edit the FortiAnalyzer VM IP address:

1. In the toolbar select *Asset* > *Manage/View Products* to open the *View Products* page.
2. Select the FortiAnalyzer VM serial number to open the *Product Details* page.
3. Select *Edit* to change the description, partner information, and IP address of your FortiAnalyzer VM from the *Edit Product Info* page.



4. Enter the new IP address then select *Save*.

You can change the IP address five (5) times on a regular FortiAnalyzer VM license. There is no restriction on a full evaluation license.

5. Select *License File Download* to save the license file (`.lic`) to your management computer. See Upload the license file on page 47 for instructions on uploading the license file to your FortiAnalyzer VM via the GUI.

Deployment package

FortiAnalyzer VM deployment packages are included with firmware images on the Customer Service & Support site. The following table list the available VM deployment packages.

VM Platform	Deployment File
Amazon Web Service AMI, EC2, and EBS	The 64bit Amazon Machine Image (AMI) is available in the AWS marketplace.
Microsoft Azure	The Microsoft Azure based VM is available in the Azure portal.
Citrix XenServer 6.2	`FAZ_VM64_XEN-v5-buildxxxx-FORTINET.out-.CitrixXen.zip`
Linux KVM RedHat 6.5	`FAZ_VM64_KVM-v5-buildxxxx-FORTINET.out-.kvm.zip`
Microsoft Hyper-V Server 2008 R2 and 2012	`FAZ_VM64_HV-v5-buildxxxx-FORTINET.out-.hyperv.zip`
Open Source XenServer 4.2.5	`FAZ_VM64_XEN-v5-buildxxxx-FORTINET.out-.OpenXen.zip`
VMware ESX 4.0 and 4.1 VMware ESXi 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0	ESX/ESXi server: `FAZ_VM64-v5-buildxxxx-FORTINET.out.ovf.zip`

For more information see the FortiAnalyzer VM datasheet available on the Fortinet web site:

https://www.fortinet.com/products/management/fortianalyzer.html.

Firmware image FTP directories are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the `FAZ_VM64_HV-v5-buildxxxx-FORTINET.out.hyperv.zip` image, found in the 5.4.0 directory, is specific to the 64bit Microsoft Hyper-V Server virtualization environment.

You can download the *FortiAnalyzer Release Notes* and MIB file from this directory. The Fortinet Core MIB file is located in the main FortiAnalyzer 5.00 directory.

Download the `.out` file to upgrade your existing FortiAnalyzer VM installation.

To download the firmware package:

1. Log in to the Fortinet Customer Service & Support portal then, from the toolbar select *Download* > *Firmware Images*. The *Firmware Images* page opens.
2. Select *FortiAnalyzer* from the *Select Product* drop-down list, then select *Download*.
3. Browse to the appropriate directory for the version that you would like to download.
4. Download the appropriate firmware image and release notes to your management computer.
5. Extract the contents of the package to a new folder on you management computer.

Deployment package contents

Citrix XenServer

The `.out.CitrixXen.zip` file contains:

- `faz.xva`: The Citrix XenServer Virtual Appliance (XVA) binary file containing virtual hardware configuration settings.
- `ovf` folder:
  - `FortiAnalyzer.ovf`: Open Virtualization Format (OVF) template file, containing virtual hardware settings for Xen.
  - `faz.vhd`: The FortiAnalyzer VM system hard disk in VHD format.
  - `datadrive.vhd`: The FortiAnalyzer VM log disk in VHD format.

Linux KVM

The `.out.kvm.zip` file contains:

- `faz.qcow2`: TheFortiAnalyzer VM system hard disk in QCOW2 format.
  The log disk and virtual hardware settings have to be configured manually.

Microsoft Hyper-V

The `.out.hyperv.zip` file contains:

- `faz.vhd`: The FortiAnalyzer VM system hard disk in VHD format.
  The log disk and virtual hardware settings have to be configured manually.

Open Source XenServer

The `.out.OpenXen.zip` file contains:

- `faz.qcow2`: The FortiAnalyzer VM system hard disk in QCOW2 format.
  The log disk and virtual hardware settings have to be configured manually.

VMware

The `.out.ovf.zip` file contains:

- `faz.vmdk`: The FortiAnalyzer VM system hard disk in Virtual Machine Disk (VMDK) format.
- `FortiAnalyzer-VM64.ovf`: The VMware virtual hardware configuration file.
- `DATADRIVE.vmdk`: The FortiAnalyzer VM log disk in VMDK format

Deploying the appliance

Prior to deploying the FortiAnalyzer VM, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiAnalyzer VM presume that you are familiar with the management software and terminology of your VM platform.

For assistance in deploying FortiAnalyzer VM, refer to the deployment chapter in this guide that corresponds to your hypervisor environment. You may also need to refer to the documentation provided with your VM server. The deployment chapters are presented as examples because, for any particular VM server, there are multiple ways of creating a virtual machine - command line tools, APIs, alternative graphical user interface tools.

Before you start your FortiAnalyzer VM appliance for the first time, you might need to adjust virtual disk sizes and networking settings. With the exception of AWS and Azure environments, the first time you start FortiAnalyzer VM, you will have access only through the console window of your VM server environment. After you configure one network interface with an IP address and administrative access, you can access the FortiAnalyzer GUI (see GUI access on page 46).

If the FortiAnalyzer VMdoes not have a valid Logical Volume Management (LVM) configuration, the LVM service will not start automatically upon boot-up when the disk already contains data. To manually enable the service, use the `execute lvm start` CLI command.

Citrix XenServer deployment example

Once you have downloaded the `FAZ_VM64_XEN-v5-buildxxxx-FORTINET.out.CitrixXen.zip` file and extracted the files, you can create the virtual machine in your Citrix Xen environment.

The following topics are included in this section:

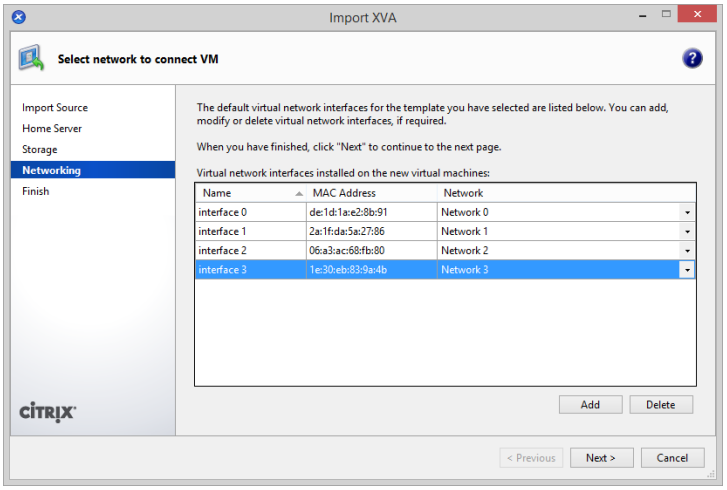
Create the virtual machine

To create the virtual machine:

1. Launch XenCenter on your management computer.

   The management computer can be any computer that can run Citrix XenServer, a Microsoft Windows application.
2. Click *ADD a server*, then enter the Citrix XenServer IP address and the root logon credentials required to manage that server.

   Your Citrix XenServer is added to the list in the left pane, and the *Virtual Machine Manager* home page opens.
3. Select *File* > *Import*.
4. Click *Browse*, locate the `faz.xva` file, select *Open*, then select *Next*.
5. Choose the pool or standalone server that will host the VM, then click *Next*.
6. Select the storage location for the FortiAnalyzer VM disk drives, then click *Next*.
7. Configure the virtual network interfaces, then click *Next*. By default, there are four virtual network interfaces.



8. Review the import settings, deselect *Start VM(s) after import*, and then click *Finish* to import the VM.

The Citrix XenServer imports the FortiAnalyzer VM files and configures the VM as specified in the template. Depending on your computer's hardware speed and resource load, as well as on the file size and speed of the network connection, this may take several minutes to complete

When the VM import is complete, the XenServer left pane will include the FortiAnalyzer VM in the list of deployed VMs for your Citrix XenServer.

Configure hardware settings

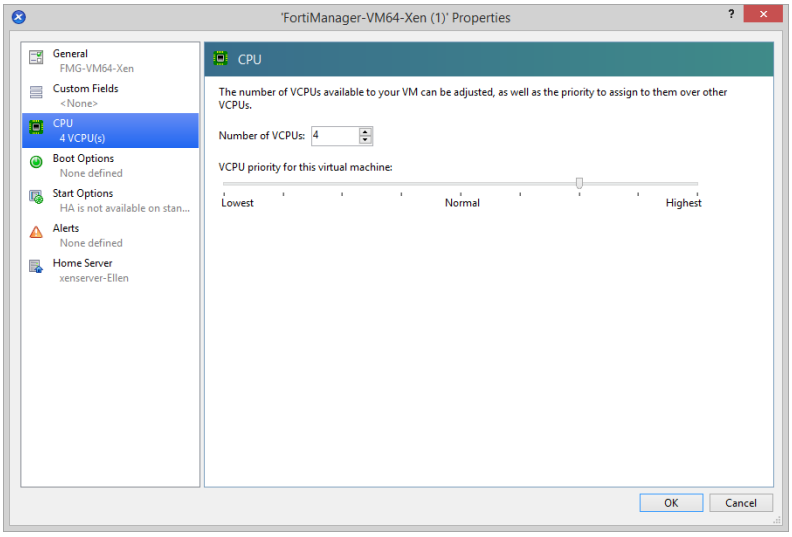
Before starting your FortiAnalyzer VM for the first time, you must adjust the VM's virtual hardware settings to meet your network requirements.

To access VM settings, open XenCenter and select the FortiAnalyzer VM in the left pane. The tabs in the right pane provide access to the virtual hardware configuration, and the console tab provides access to the FortiAnalyzer console.

Disk resizing must be done before you start the VM for the first time.
If you know your environment will expand in the future, it is recommended to add hard disks larger than the 500GB base license requirement. This will allow your environment to be expanded as required while not taking up more space than is needed.
See Licensing on page 7 for more information.

To set the number of CPUs:

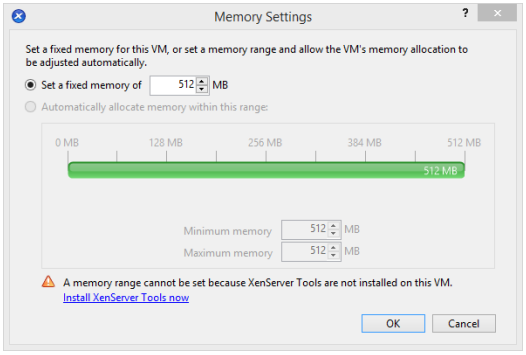
1. In the XenCenter left pane, right-click the FortiAnalyzer VM and select *Properties*.
2. In the left pane of the *Properties* window, select *CPU*.



3. Adjust the in the *Number of VCPUs*, then click *OK*.
   XenCenter will display a warning if you select more CPUs than the Xen host computer contains. Such a configuration might reduce performance.

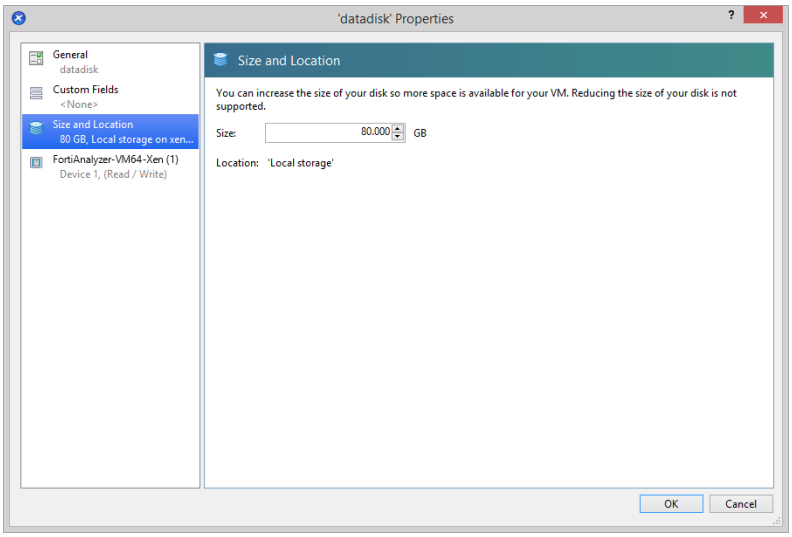
To set the memory size:

1. In the XenCenter left pane, select the FortiAnalyzer VM.
2. In the right pane, select the *Memory* tab.
3. Click *Edit* and modify the value in the *Set a fixed memory of* field. See Minimum system requirements on page 8 to determine your required memory.
4. Click *OK*.



To resize the data disk:

1. In the XenCenter left pane, select the FortiAnalyzer VM.
2. In the right pane, select the *Storage* tab.
3. Select the data disk, then click *Properties* to open the *Properties* window.
4. Select *Size and Location*.



5. Adjust the *Size* to the required value, then click *OK*. See Licensing on page 7 for more information.

The FortiAnalyzer VM allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

Start the virtual machine

You can now proceed to start on your FortiAnalyzer VM.

- In the XenCenter left pane, right-click on the name of the FortiAnalyzer VM and select *Start*.
- Select the name of the FortiAnalyzer VM from the left pane, then select *Start* in the toolbar.

Hyper-V deployment example

Once you have downloaded the `FAZ_VM64_HV-v5-buildxxxx-FORTINET.out.hyperv.zip` file and extracted the package contents to a folder on your Microsoft server, you can deploy the VHD package to your Mircosoft Hyper-V environment.

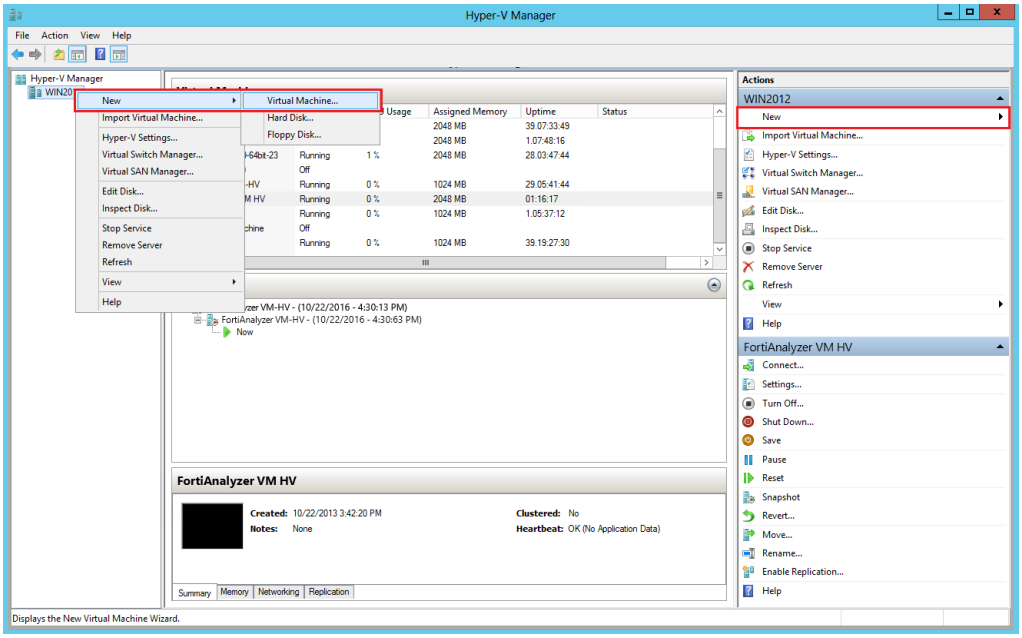
The following topics are included in this section:

- Create the virtual machine
- Configure hardware settings
- Start the virtual machine

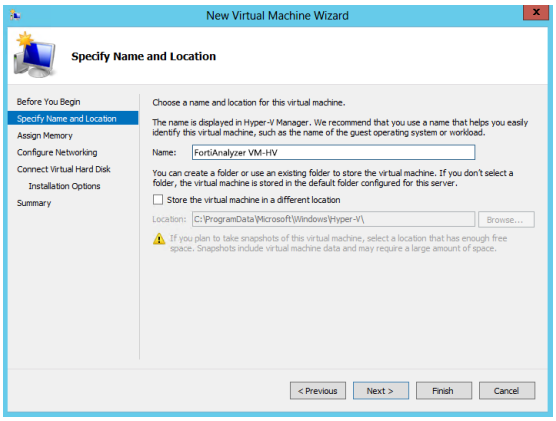
Create the virtual machine

To create the virtual machine:

1. Launch the Hyper-V Manager in your Microsoft server. The *Hyper-V Manager* home page opens.
2. Select the server in the right-tree menu. The server details page opens.

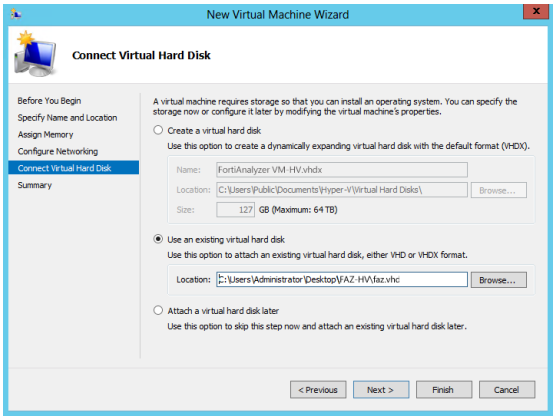


3. Right-click the server and select *New* > *Virtual Machine*, or in the *Actions* menu, select *New* > *Virtual Machine*. The *New Virtual Machine Wizard* opens.
4. Click *Next* to create a virtual machine with a custom configuration. The *Specify Name and Location* page opens.



5. Enter a name for this VM. The name is displayed in the Hyper-V Manager.
6. Click *Next* to continue to the *Assign Memory* page .
7. Specify the amount of memory to allocate to this virtual machine. See Minimum system requirements on page 8 to determine your required memory.
8. Click *Next* to continue to the *Configure Networking* page.
9. You must configure network adapters in the *Settings* page.

   Each new VM includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. FortiAnalyzer VM requires four network adapters.
10. Select *Next* to continue to the *Connect Virtual Hard Disk* page.

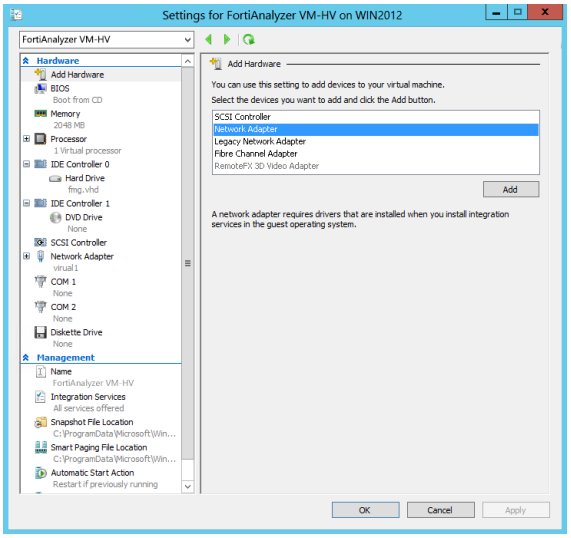


11. Select to use an existing virtual hard disk and browse for the `faz.vhd` file that you downloaded from the Fortinet Customer Service & Support portal.
12. Select *Next* to continue to the *Summary* page.
13. To create the virtual machine and close the wizard, select *Finish*.

Configure hardware settings

Before powering on your FortiAnalyzer VM you must configure the virtual processors, memory, network adapters, and hard disk to match your FortiAnalyzer VM license. See Licensing on page 7 for FortiAnalyzer VM license information.

To open the *Settings* page, in the Hyper-V Manager, right-click on the name of the virtual machine and select *Settings*, or select the virtual machine then click *Settings* from the *Actions* menu.

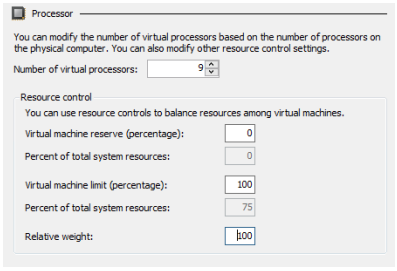


To configure virtual memory:

1. In the *Settings* page, select *Memory* from the *Hardware* menu. The *Memory* page is displayed.
2. Configure the memory for the VM. See Minimum system requirements on page 8 to determine your required memory.
3. Click *Apply* to save your settings.

To configure virtual processors:

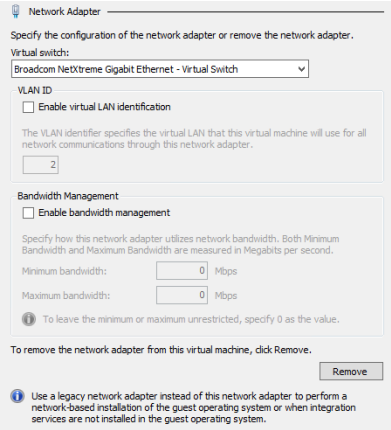
1. In the *Settings* page, select *Processor* from the *Hardware* menu. The *Processor* page is displayed.



2. Configure the number of virtual processors for the VM. Optionally, you can use resource controls to balance resources among VMs.
3. Click *Apply* to save your settings.

To configure network adapters:

1. In the *Settings* page, select *Add Hardware* from the *Hardware* menu.
2. From the device list, select *Network Adapter*, then click *Add*. The *Network Adapter* page opens.



3. Manually configure four network adapters in the settings page. For each network adapter, select a virtual switch from the drop-down list.
4. Click *Apply* to save your settings.

To configure the virtual hard disk:

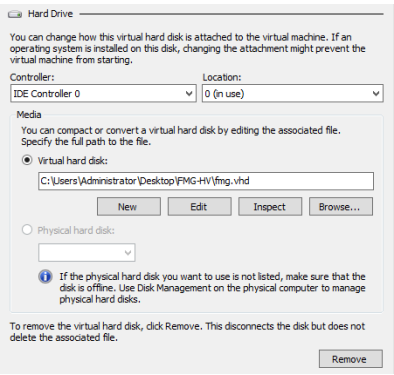
The FortiAnalyzer VM requires at least two virtual hard disks. Before powering on the FortiAnalyzer VM, you must add at least one more virtual hard disk. The default hard drive, `faz.vhd`, contains the operating system. The second hard drive is used for logs.

If you know your environment will expand in the future, it is recommended to add hard disks larger than the 500GB base license requirement. This will allow your environment to be expanded as required while not taking up more space in the Storage Area Network (SAN) than is needed. See Licensing on page 7 for more information.

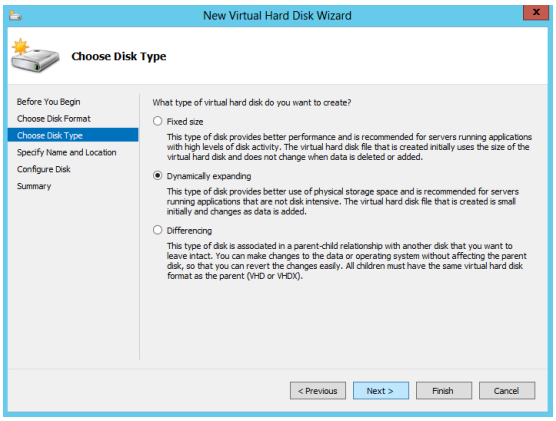
The FortiAnalyzer VM allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

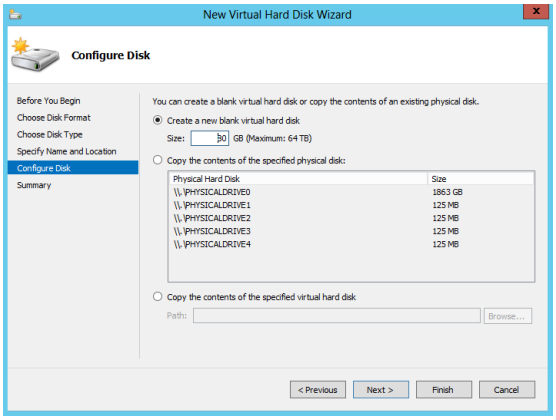
1. In the *Settings* page, select *IDE Controller 0* from the *Hardware* menu.
2. Select the type of drive that you want to attach to the controller, then click *Add*. The *Hard Drive* page opens.



3. Click *New* to create a new virtual hard disk. The *New Virtual Hard Disk Wizard* opens to help you create a new virtual hard disk.
4. Click *Next* to continue to the *Choose Disk Format* page.
5. Select to use VHDX format virtual hard disks. This format supports virtual disks up to 64TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier that Windows Server 2012.
6. Click *Next* to continue to the *Choose Disk Type* page.



7. Select the type of virtual disk you want to use, one of the following:
   - *Fixed Size*: This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.
   - *Dynamically Expanding*: This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual disk file that is created is small initially and changes as data is added.
   - *Differencing*: This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).
8. Click *Next* to continue to the *Specify Name and Location* page.
9. Specify the name and location of the virtual hard disk file. Use the *Browse* button to select a specific file folder on your server.
10. Click *Next* to continue to the *Configure Disk* page.



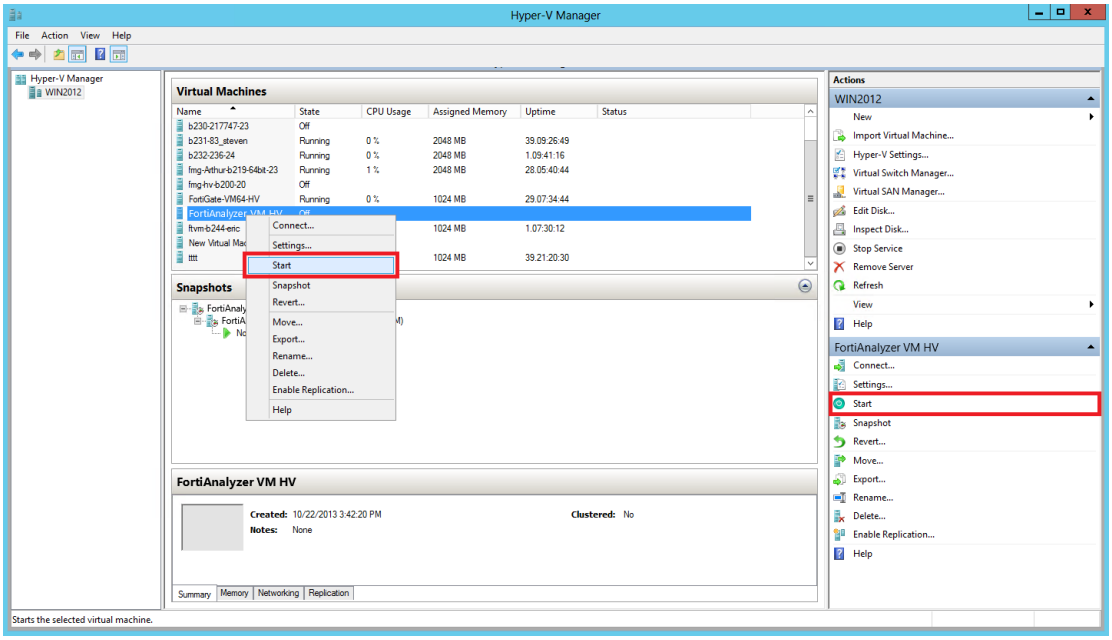
11. Select *Create a new blank virtual hard disk*, then enter the size of the disk in GB. The maximum size is dependent on your server environment.
12. Click *Next* to continue to the *Summary* page.

    The summary page provides details about the virtual hard disk.
13. Click *Finish* to create the virtual hard disk, then click *Apply* to save the settings, and then click *OK* to exit the settings page.

Start the virtual machine

You can now proceed to power on your FortiAnalyzer VM.

- In the list of virtual machines, right-click on the name of the FortiAnalyzer VM and select *Start*.
- Select the name of the FortiAnalyzer VM from the list of virtual machines, then click *Start* from the *Actions* menu.



KVM deployment example

Once you have downloaded the `FAZ_VM64_KVM-v5-buildxxxx-FORTINET.out.kvm.zip` file and extracted the virtual hard drive image file, you can create the virtual machine in your KVM environment.

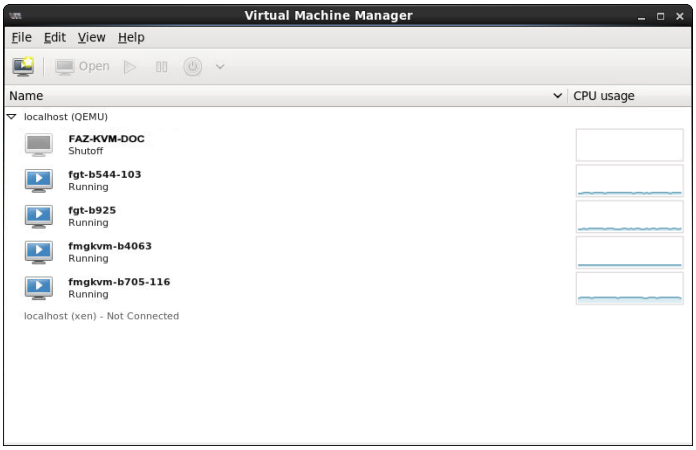
The following topics are included in this section:

- Create the virtual machine
- Configure hardware settings
- Start the virtual machine

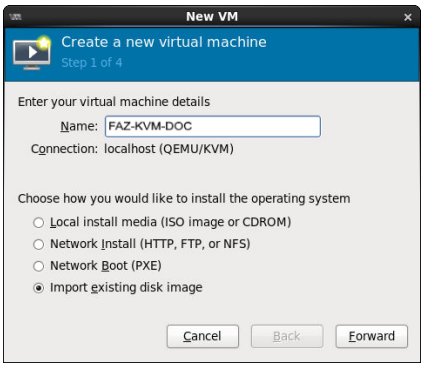
Create the virtual machine

To create the virtual machine:

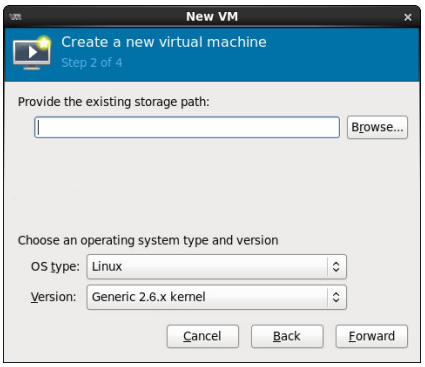
1. Launch Virtual Machine Manager (virt-manager) on you KVM host server. The *Virtual Machine Manager* home page opens.



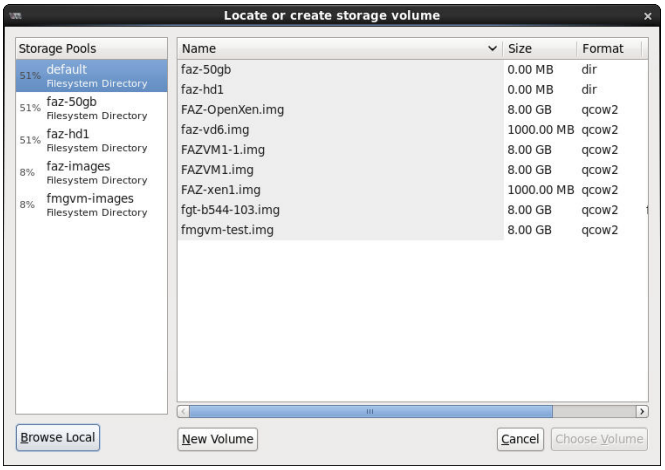
2. Select *Create a new virtual machine* from the toolbar..



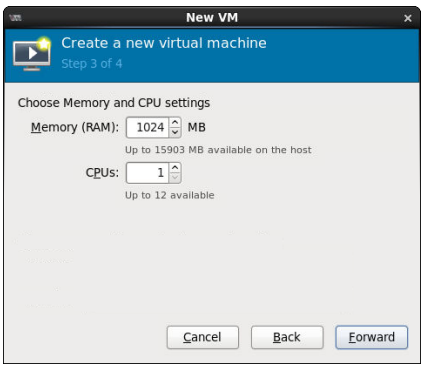
3. Enter a name for the virtual machine, such as *FAZ-KVM-DOC*.
4. Ensure that *Connection* is *localhost*, select *Import existing disk image*, then click *Forward* to continue.



5. In the *OS Type* field select *Linux*.
6. In the *Version* field select *Generic 2.6.x kernel*. You may have to first select *Show all OS options*.
7. Click *Browse* to locate the storage volume.



8. If you copied the *faz.qcow2* file to `/var/lib/libvirt/images` it will be shown on the right. If you saved it elsewhere on the server, click *Browse Local* to find it.
9. Once the file has been located, click *Choose Volume*, then click *Forward*.



10. Specify the amount of memory and the number of CPUs to allocated to this VM, then select *Forward*. See Minimum system requirements on page 8 to determine your required memory.
11. Expand the *Advanced options* section. By default, a new virtual machine includes one network adapter. Select a network adapter on the host computer.

    Optionally, set a specific MAC address for the virtual network interface.

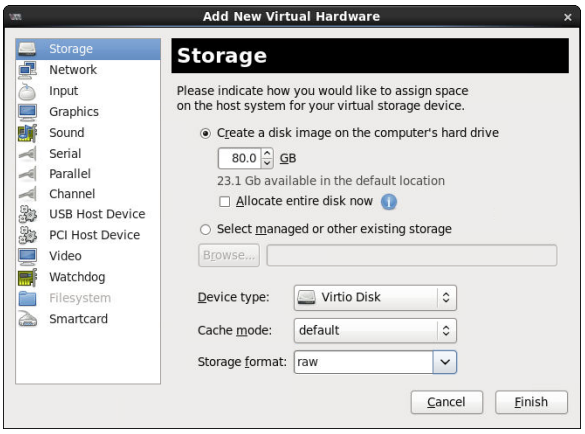
12. Set *Virt Type* to *virtio* and set *Architecture* to *qcow2*.
13. Click *Finish* to create the VM.

Configure hardware settings

Before powering on your FortiAnalyzer VM you must configure virtual disks and at least four network interfaces.

To configure settings on the server:

1. In the Virtual Machine Manager, locate the name of the VM, then select *Open* from toolbar.
2. In the Virtual Machine window, select *Show virtual hardware details*.
3. Click *Add Hardware* to open the *Add Hardware* window
4. Select *Storage*.



5. Select *Create a disk image on the computer's harddrive*, and set the size to 80GB.

If you know your environment will expand in the future, or if you will be using ADOMs, it is recommended to add hard disks larger than 500GB. This will allow your environment to be expanded as required while not taking up more space than is needed. See Licensing on page 7 for more information.

The FortiAnalyzer VM allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

6. Enter the following information:

Device Type	Virtio disk
Cache mode	writethrough
Storage format	raw

7. Select *Network* to add more network interfaces. The *Device Model* must be *Virtio*.

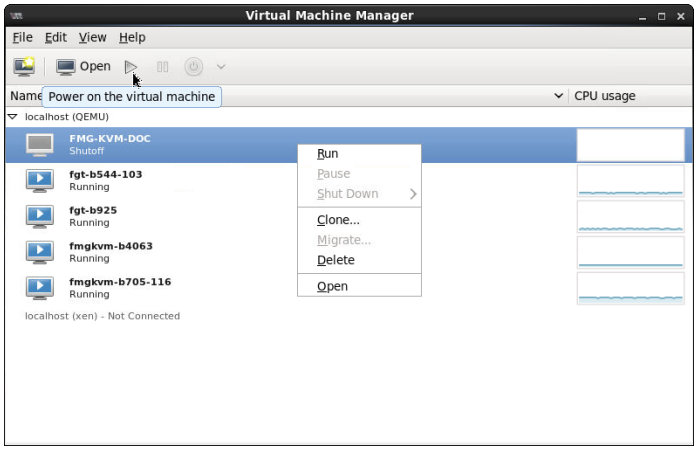
A new VM includes one network adapter by default. More can be added through the *Add Hardware* window. FortiAnalyzer VM supports up to four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.

8. Click *Finish*.

Start the virtual machine

You can now proceed to power on your FortiAnalyzer VM.

- Right-click on the FortiAnalyzer VM and select Run, or
- Select the FortiAnalyzer VM from the list of VMs, then click *Power on the virtual machine* from the toolbar.



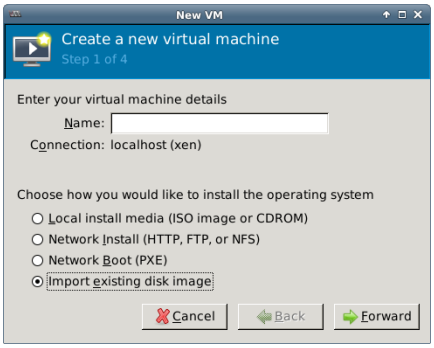
Open Xen deployment example

Once you have downloaded the `FAZ_VM64_XEN-v5-buildxxxx-FORTINET.out.OpenXen.zip` file and extracted the *faz.qcow2*, you can create the virtual machine in your Open Xen environment.

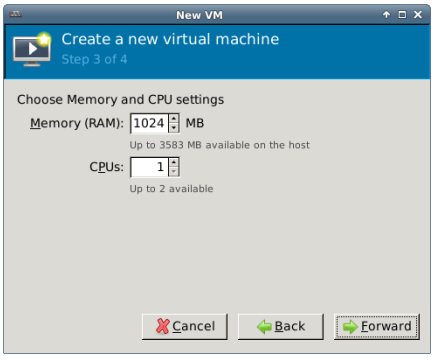
Create and configure the virtual machine

To deploy and configure the virtual machine:

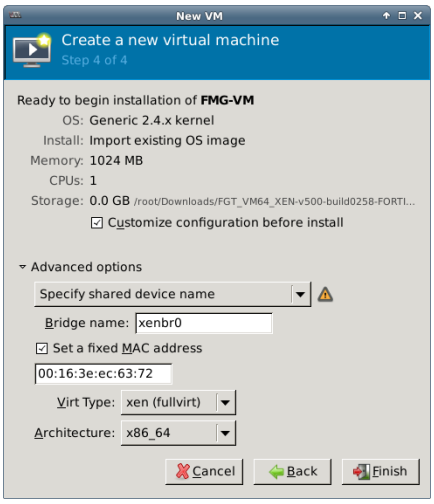
1. Launch Virtual Machine Manager (virt-manager) on you Open Xen host server. The *Virtual Machine Manager* home page opens.
2. Select *Create a new virtual machine* from the toolbar..



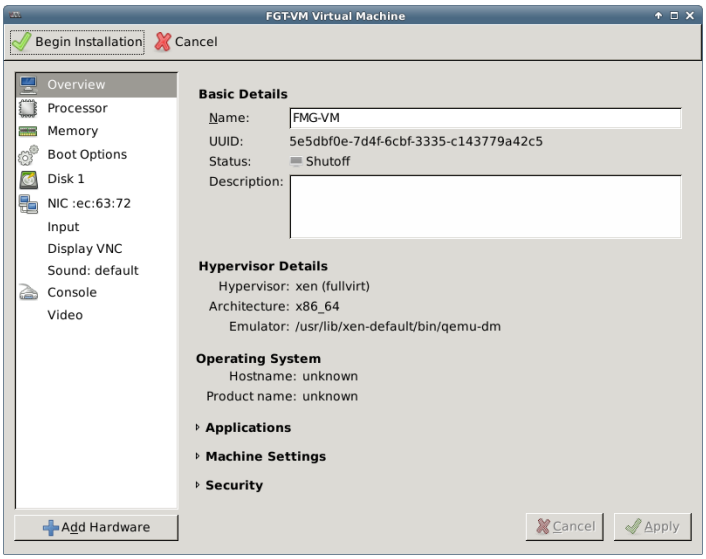
3. Enter a name for the VM, such as *FAZ-VM*.
4. Ensure that *Connection* is *localhost*, select *Import existing disk image*, then click *Forward* to continue.
5. In the *OS Type* field select *Linux*. In the *Version* field select *Generic 2.6.x kernel*.
6. Click *Browse* to open the *Locate or create storage volume* window.
7. Click *Browse Local*, find the faz.qcow2 disk image file, then click *Choose Volume* and then *Forward*.



8. Specify the amount of memory and the number of CPUs to allocated to this VM. See Minimum system requirements on page 8 to determine your required memory.
9. Click *Forward*.



10. Select *Customize configuration before install*. This enables you to make hardware configuration changes before the VM creation is started.
11. Expand the *Advanced options* section.
    - By default, a new virtual machine includes one network adapter.
    - Select *Specify shared device name*, and enter the name of the bridge interface on the Open Xen host.
    - Optionally, set a fixed MAC address for the virtual network interface.
    - *Virt Type* and *Architecture* are set by default and should not need to be changed.
12. Click *Finish*. The virtual machine hardware configuration window opens. It can be used to add hardware such as network interfaces and disk drives.



13. Click *Add Hardware* to open the *Add Hardware* window, then click *Storage*.
14. Select *Create a disk image on the computer's harddrive*, and set the size to an appropriate size.

If you know your environment will expand in the future, or if you will be using ADOMs, it is recommended to add hard disks larger than 500GB. This will allow your environment to be expanded as required while not taking up more space than is needed. See Licensing on page 7 for more information.

The FortiAnalyzer VM allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

15. Select *Network* to add more network interfaces.

    A new VM includes one network adapter by default. More can be added through the *Add Hardware* window. FortiAnalyzer VM required four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.

16. Click *Finish*.
17. Click *Begin Installation*.

    After the installation completes successfully, the VM will start and the console window will open.

VMware deployment example

The FortiAnalyzer VM can be deployed and configured using VMware vSphere Hypervisor™ (ESX/ESXi) and VMware vSphere Client™.

VMware vSphere

Once you have downloaded the `FAZ_VM64-v5-buildxxxx-FORTINET.out.ovf.zip` file and extracted the package contents to a folder on your management computer, you can deploy the OVF package to your VMware environment.

Prior to deploying the FortiAnalyzer VM, ensure that the following are configured and functioning properly:

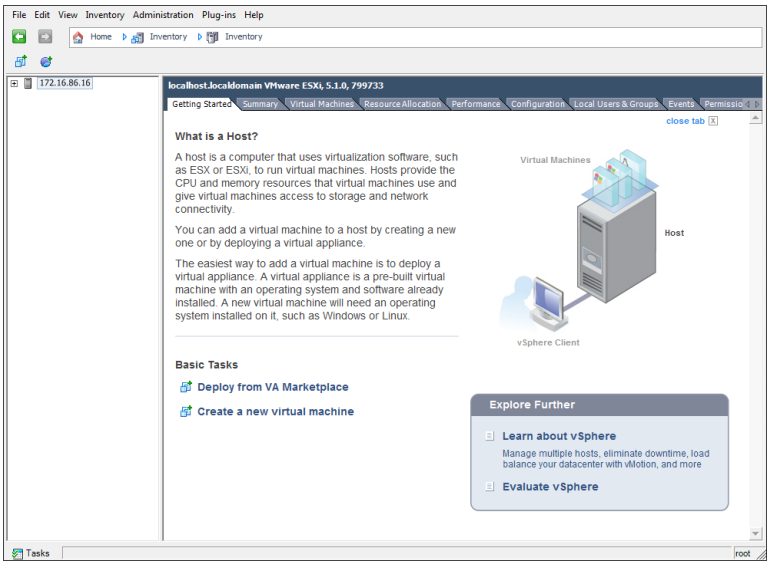
- VMware vSphere Hypervisor™ (ESX/ESXi) software must be installed on a server and updated to the latest patch release prior to installing FortiAnalyzer VM. Go to http://www.vmware.com/products/vsphere-hypervisor/index.html for installation details.
- VMware vSphere Client™ must be installed on the computer that you will be using for managing the FortiAnalyzer VM.

The following topics are included in this section:

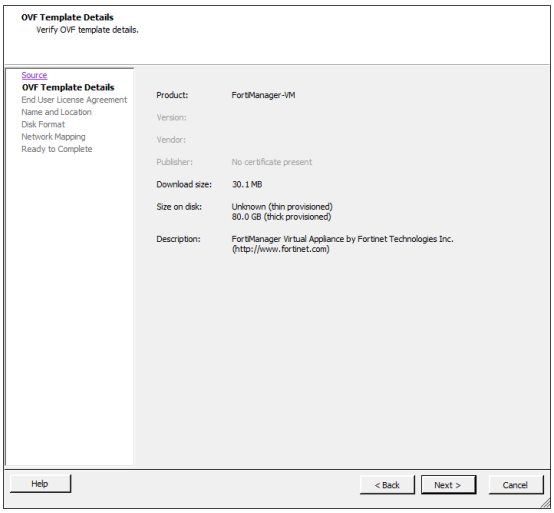
Deploy the OVF file

To deploy the OVF file template:

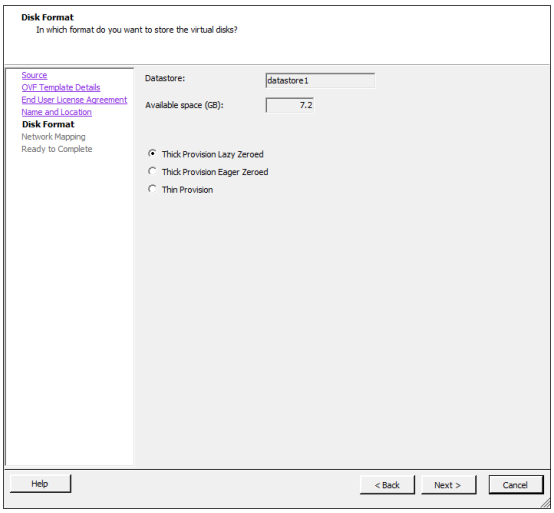
1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password, then click *Login*. The vSphere client home page opens.



2. Select *File* > *Deploy OVF Template* to launch the OVF Template wizard. The OVF Template *Source* page opens.
3. Click *Browse*, locate the OVF file on your computer, then click *Next* to continue. The OVF Template *Details* page opens.



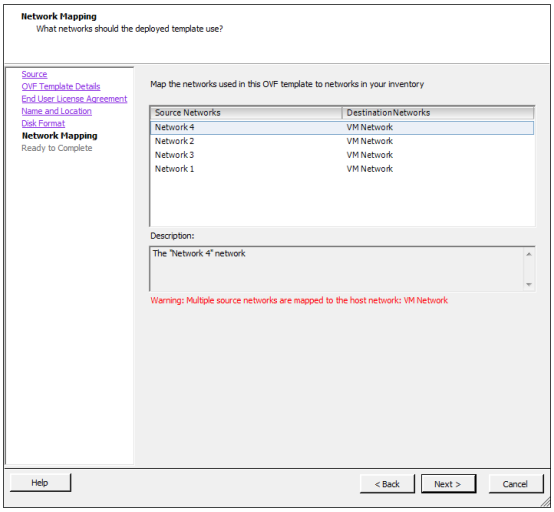
4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Click *Next* to continue. The OVF Template *End User License Agreement* page opens.
5. Read the end user license agreement, then click *Accept* then *Next* to continue. The OVF Template *Name and Location* page opens.
6. Enter a name for this OVF template. The name can contain up to 80 characters and it must be unique within the inventory folder. Click *Next* to continue. The OVF Template *Disk Format* page opens.



7. Select one of the following:
   - *Thick Provision Lazy Zeroed*: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
   - *Thick Provision Eager Zeroed*: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
   - *Thin Provision*: Allocates the disk space only when a write occurs to a block, but the total volume size is reported by the Virtual Machine File System (VMFS) to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains in the volume regardless of if you have deleted data, etc.

If you know your environment will expand in the future, it is recommended to add hard disks larger than the FortiAnalyzer VM base license requirement and utilize *Thin Provision* when setting the OVF Template disk format. This will allow your environment to be expanded as required while not taking up more space in the SAN than is needed.

8. Click *Next* to continue. The OVF Template *Network Mapping* page opens.



9. Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiAnalyzer VM. You must set the destination network for this entry to access the device console. Click *Next* to continue. The OVF Template *Ready to Complete* page opens.
10. Review the template configuration.

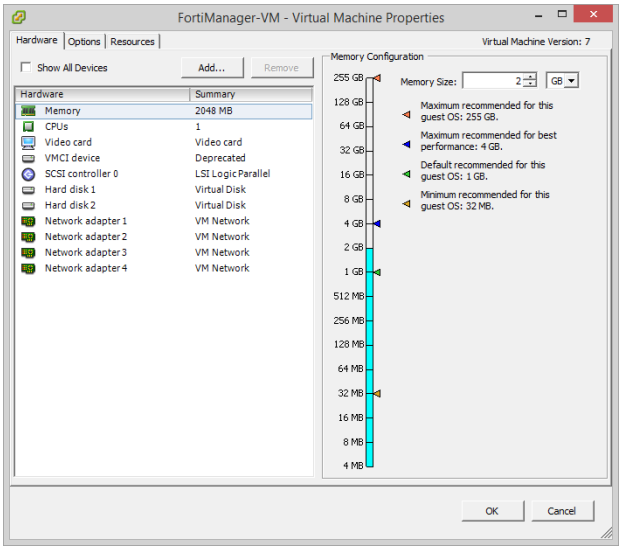
    Ensure that *Power on after deployment* is not enabled. You might need to configure the FortiAnalyzer VM hardware settings prior to powering on the VM.
11. Click *Finish* to deploy the OVF template. You will receive a *Deployment Completed Successfully* dialog box once the FortiAnalyzer VM OVF template wizard has finished.

Configure hardware settings

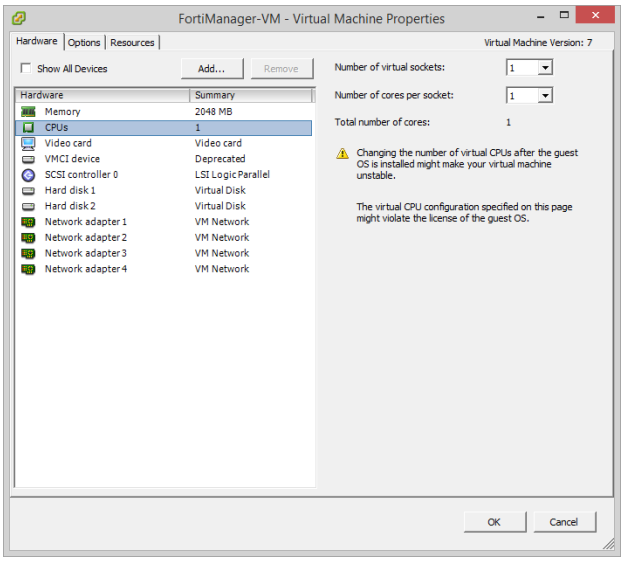
Before powering on your FortiAnalyzer VM you must configure the virtual memory, virtual CPU, and virtual disk.

To configure the VM:

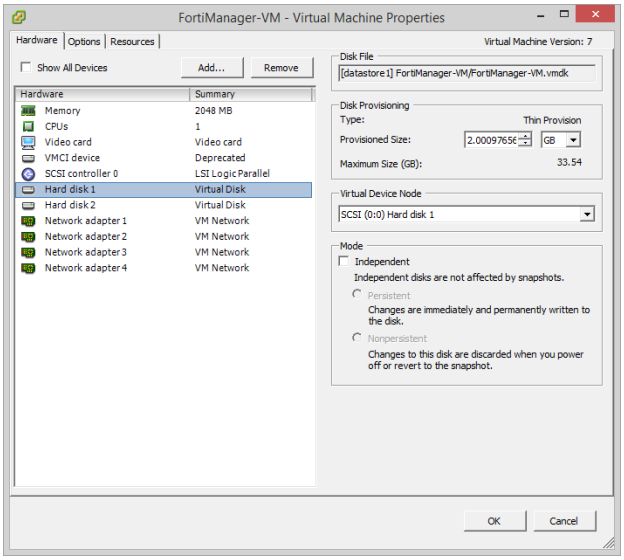
1. In the vSphere Client, right-click on the FortiAnalyzer VM in the left pane and select *Edit Settings* to open the *Virtual Machine Properties* window.
2. Select *Memory* from the *Hardware* list, then adjust the *Memory Size* as required. See Minimum system requirements on page 8 to determine your required memory.



3. Select *CPUs* from the *Hardware* list, then adjust the *Number of virtual sockets* and *Number of cores per socket* as required.



4. Select *Hard disk 2*, the log disk, from the *Hardware* list, and configure it as required. *Hard disk 1* should not be edited.



The FortiAnalyzer VM allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

5. Click *OK* to apply your changes.

Power on the virtual machine

You can now proceed to power on your FortiAnalyzer VM.

- Select the FortiAnalyzer VM in the left pane and click *Power on the virtual machine* in the *Getting Started* tab.
- Select the VM in the left pane, then click *Power On* in the toolbar.
- Right-click the VM in the left pane, then select *Power* > *Power On* from the right-click menu.

Azure deployment example

FortiAnalyzer VM can be deployed on Microsoft Azure. Prior to deploying the VM, the following are required:

- Microsoft Azure subscription
- Virtual network
- Storage account

Deploy the virtual machine

This section shows the steps for deploying the FortiAnalyzer VM from your Microsoft Azure dashboard.

To deploy the VM:

1. Log in to your Azure account.
2. Click *New* in the option pane
3. Enter *FortiAnalyzer* in the search field on the *New* blade, then click *Fortinet FortiAnalyzer for Azure* in the results list.
4. In the FortiAnalyzer VM blade, confirm that the deployment model is correct, then click *Create*.
5. Fill out the basic configuration settings:

VM Name	Enter a name for the virtual appliance.
Administrative Username	Enter the administrative name for the VM. It cannot be `admin`.
Password	Enter then confirm the admin account password. The password must be between 6 and 72 characters long, and contain characters from 3 of: uppercase characters, lowercase characters, numbers, and special characters.
Subscription	Optionally, select a subscription from the drop-down list.
Resource Group	Enter a current Resource Group for the VM, or create a new group.
Location	Optionally, select a location from the drop-down list.

6. Click *OK* to proceed to the network and storage setting. Configure the following:

Virtual network	Select a current virtual network, or create a new one.
Subnets	Confirm or customize the subnet for the VM, including: • Outside Subnet name • Outside Subnet address prefix • Inside Subnet name • Inside Subnet address prefix

Virtual machine size	Select the size of the VM to provision. At least *Standard A2*, with 3.5GB of RAM and two disks, must be selected.
Storage Account	Select a storage account, or create a new account, to contain the disk drives of the VM.

7. Click *OK* to proceed to the IP assignment setting. Configure the following:

Public IP address name	Enter the public IP address name, or create a new one.
Domain name label	Enter the DNS prefix to use for the public IP address.
Public IP Address Type	Select if the IP address is static or dynamic.
Outside Address	Confirm or customize the IP address of the outside interface of the VM.
Inside Address	Confirm or customize the IP address of the inside interface of the VM.

8. Click *OK* to proceed to the *Summary* blade. If the VM fails validation, correct the errors and try again.
   Click *Download template* to download the VM template as a JSON file.
9. Click *OK* to open the *Create* blade.
10. Read the terms of use and privacy policy, then click *Create* to create the VM.
11. To connect to the FortiAnalyzer VM GUI, open a web browser and use the public DNS address as the URL:
    ```
    https://<public DNS address>
    ```
12. Log in with the configured administrative username and password to configure your FortiAnalyzer VM.

AWS deployment example

FortiAnalyzer VM can be deployed on the AWS Elastic Compute Cloud (EC2). Prior to deploying the VM, the following are required:

- Amazon EC2 account

The FortiAnalyzer VM can be deployed using either the AWS Marketplace *1-Click Launch* option, or directly from the EC2 console.

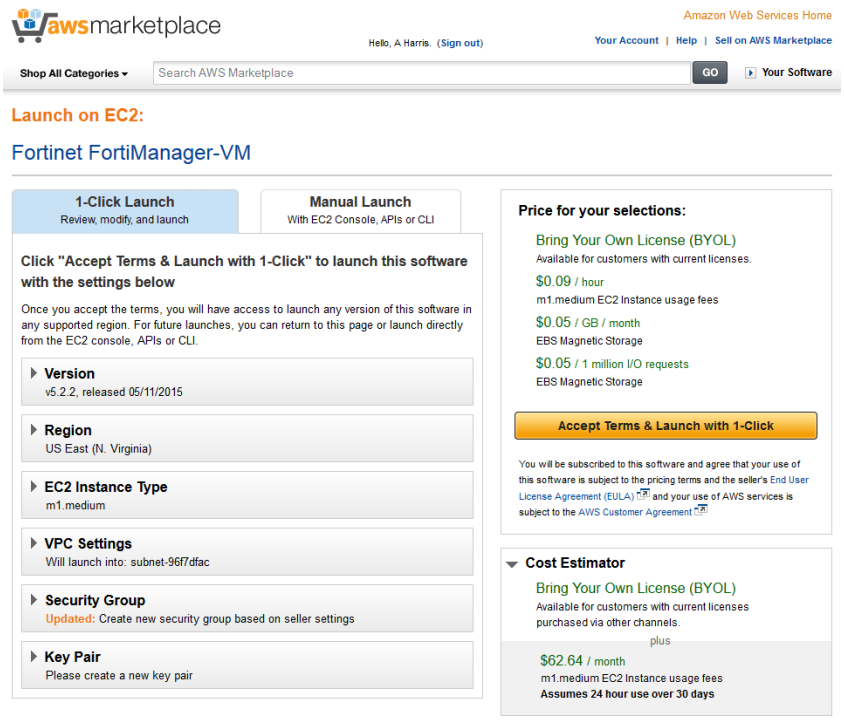
This chapter includes the following sections:

AWS Marketplace 1-Click Launch

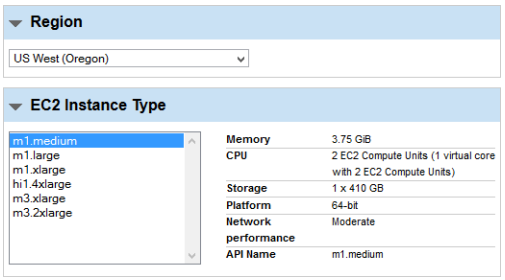
This section shows the steps for deploying the FortiAnalyzer VM from the AWS Marketplace using the *1-Click Launch* option.

To deploy the VM from the AWS Marketplace:

1. Log in to AWS.
2. From the AWS Marketplace, find the Fortinet FortiAnalyzer-VM page by searching with the key word *Fortinet*, or by selecting *Security* in the left pane.
3. On the FortiAnalyzer VM page, click *Continue*.

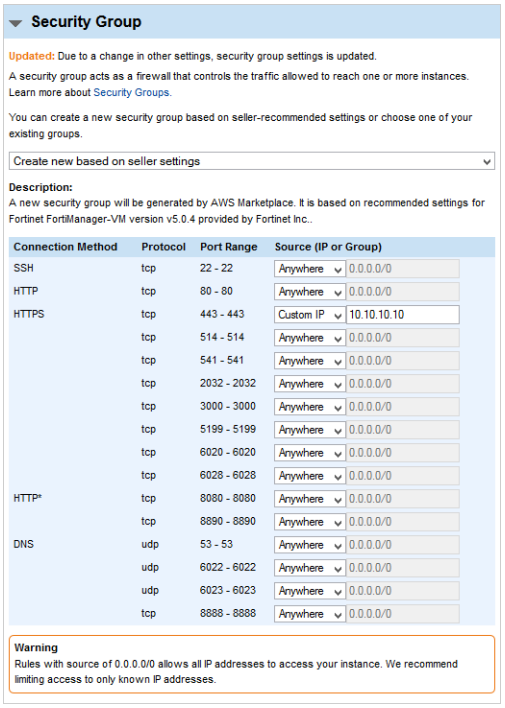


4. Select a region and the instance type. Ensure that the instance type fits the size of your deployment and potential future growth.

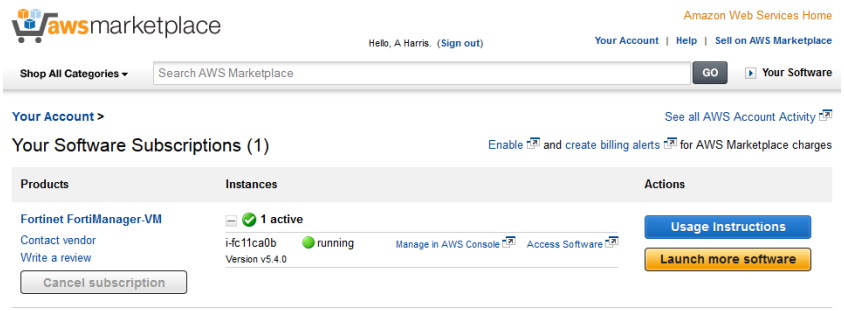


5. Under *Security Group*, ensure that *Create new based on seller settings* is selected from the drop-down list

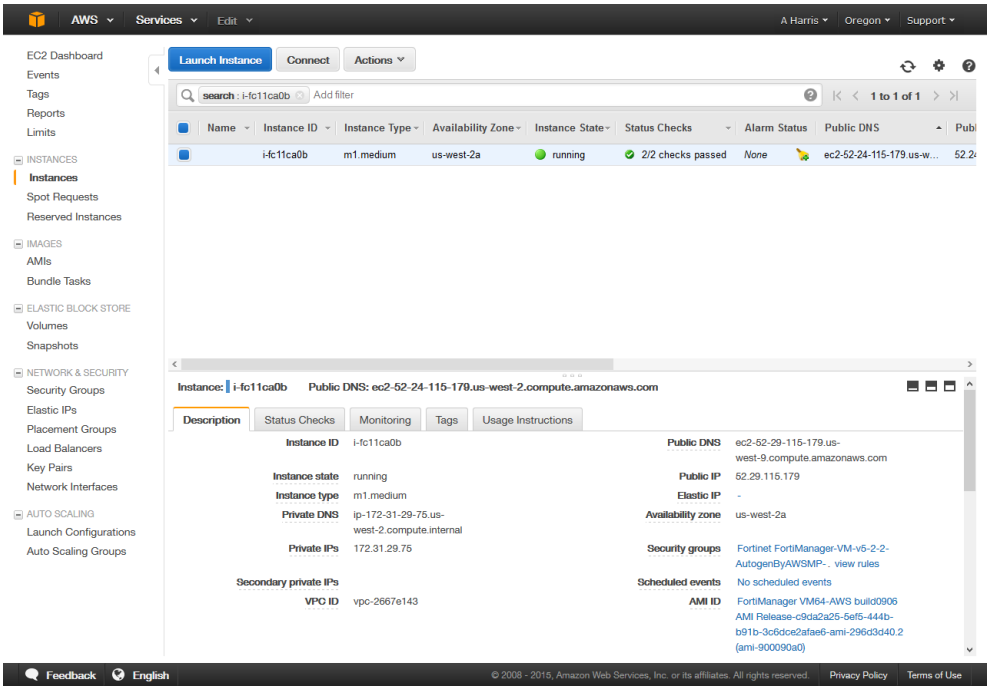
   The only open port that is required for the initial configuration of the VM is port 443, which will allow for an HTTPS connections to the GUI. The remaining ports can also be opened to allow for all potential FortiAnalyzer communication.



6. Use the instructions provided under *Key Pair* to create a new key pair, or use an existing key pair if it is secure.
7. Click *Accept Terms & Launch with 1-Click* to deploy the instance and view the summary page.
8. Close the summary page, then, from the software subscriptions page, click *Manage in AWS Console* to view the VM instance and the public DNS address.



The public DNS address is used to connect to and configure the FortiAnalyzer VM via the GUI.



9. To connect to the FortiAnalyzer VM GUI, open a web browser and use the public DNS address as the URL:
   `https://<public DNS address>`
10. Log in with default username `admin` and the instance ID as the password to configure your FortiAnalyzer VM.

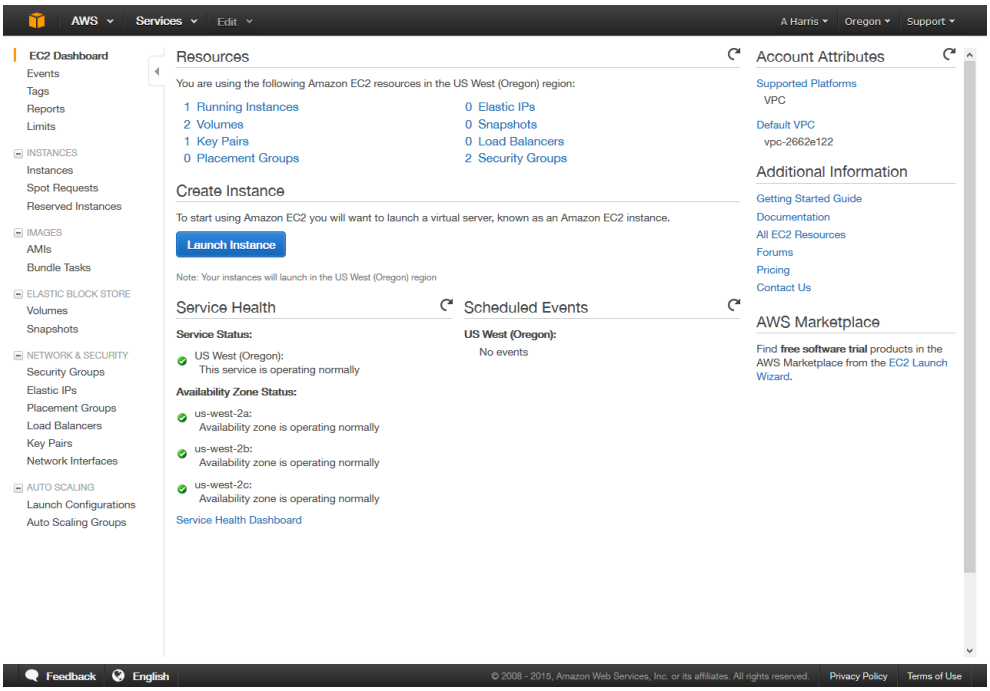
In FortiAnalyzer VM 5.4.1 and earlier, if the instance ID is a long ID (19 characters), only the first 10 characters are used as the default password.

AWS EC2 console

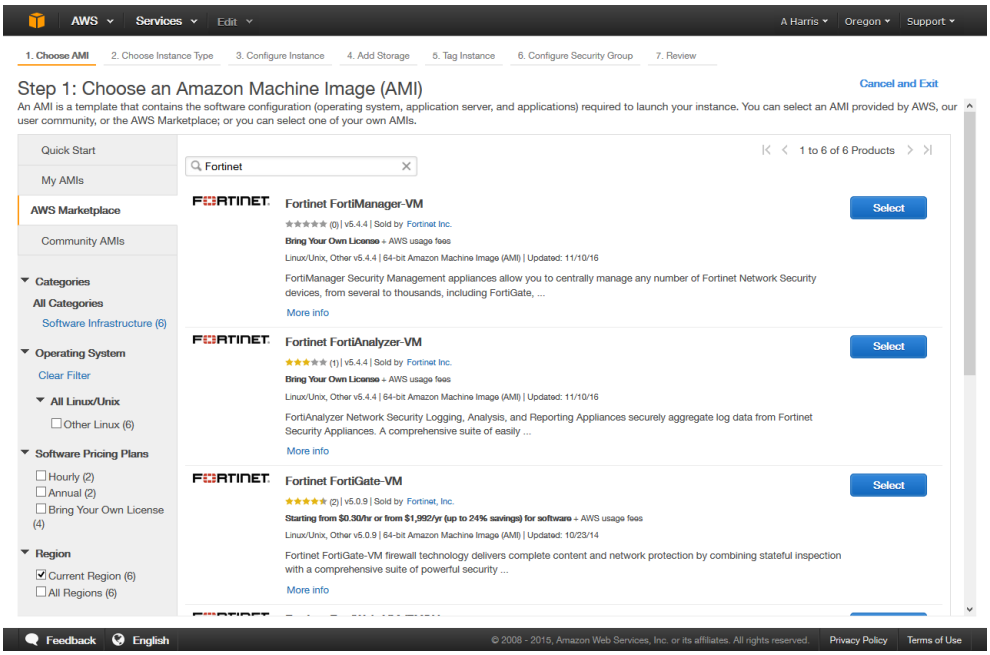
This section shows the steps for deploying the FortiAnalyzer VM directly from the EC2 console.

To deploy the VM from the EC2 console:

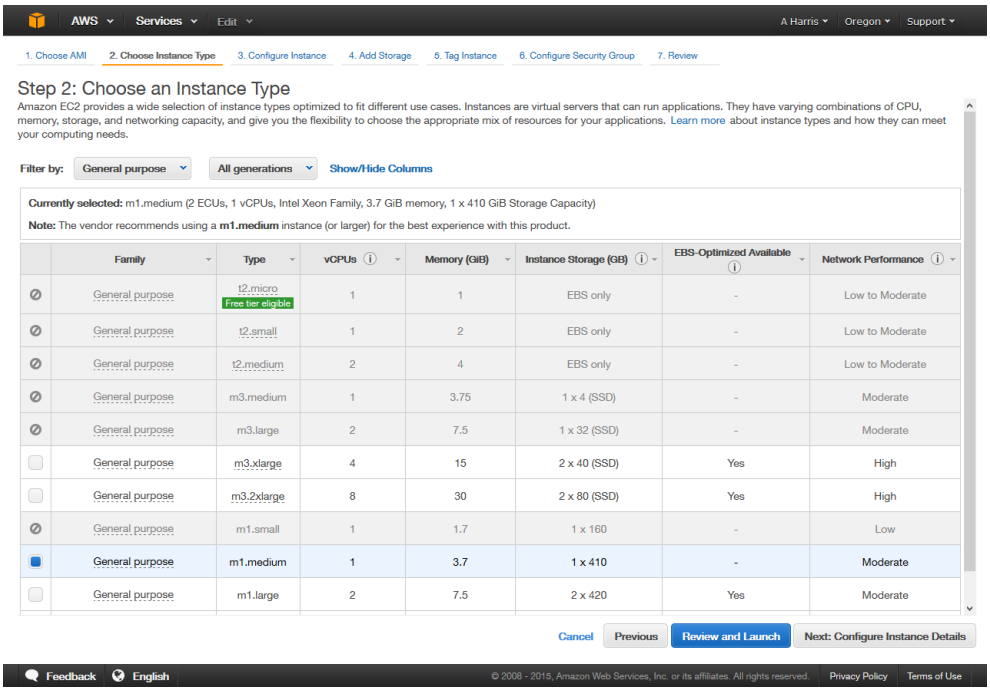
1. Log in to AWS and go to your EC2 dashboard.



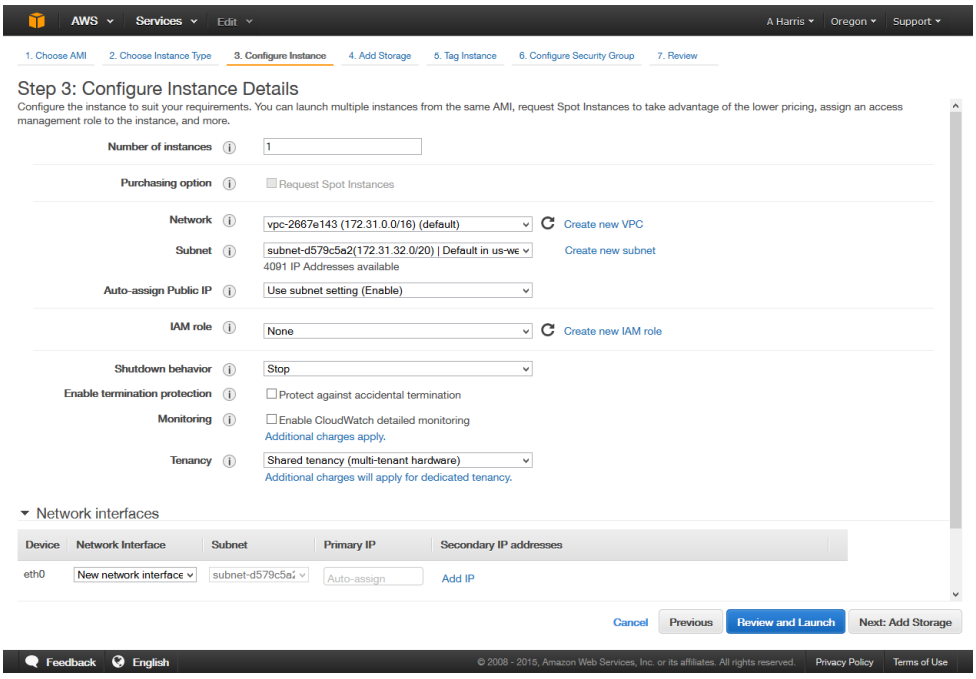
2. Click *Launch Instance* to choose an Amazon Machine Image (AMI).
   Select the *AWS Marketplace* category, then search for *Fortinet*.



3. *Select* the FortiAnalyzer VM, and then choose the instance type that matches your license.

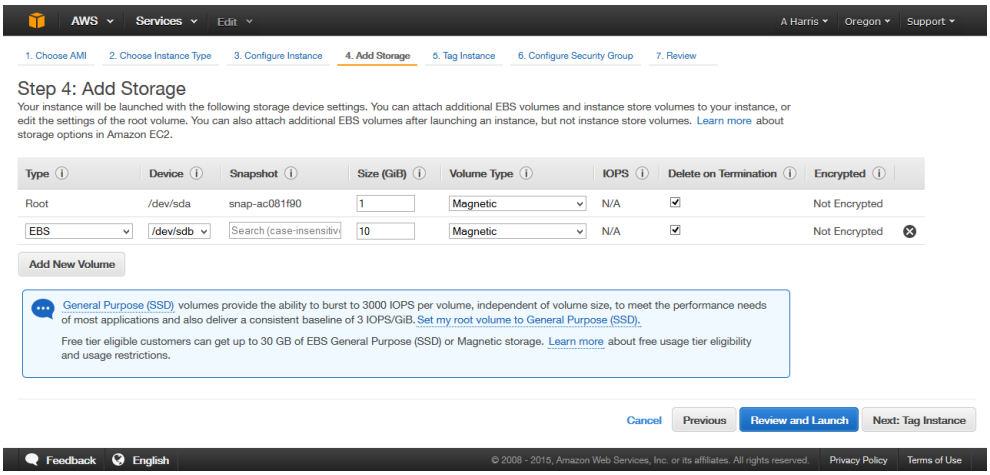


4. Click *Next: Configure Instance Details* to configure the instance details, including the public subnet and network interfaces.

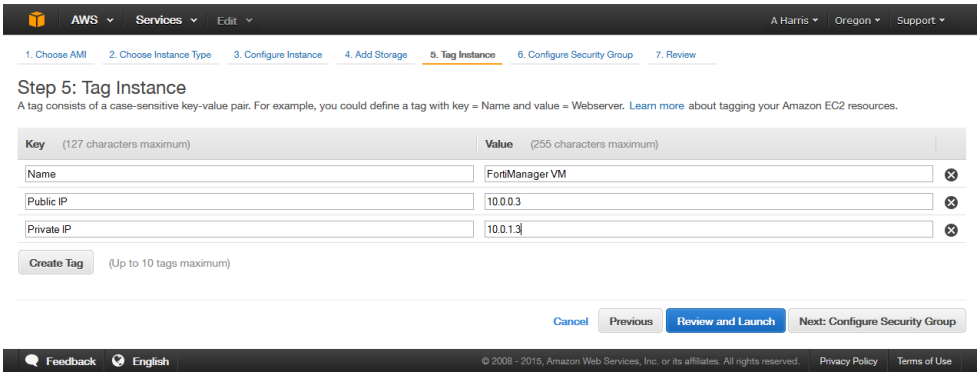


A network interface must be manually created so that you can upload your license file. Up to two interfaces can be attached to the instance.

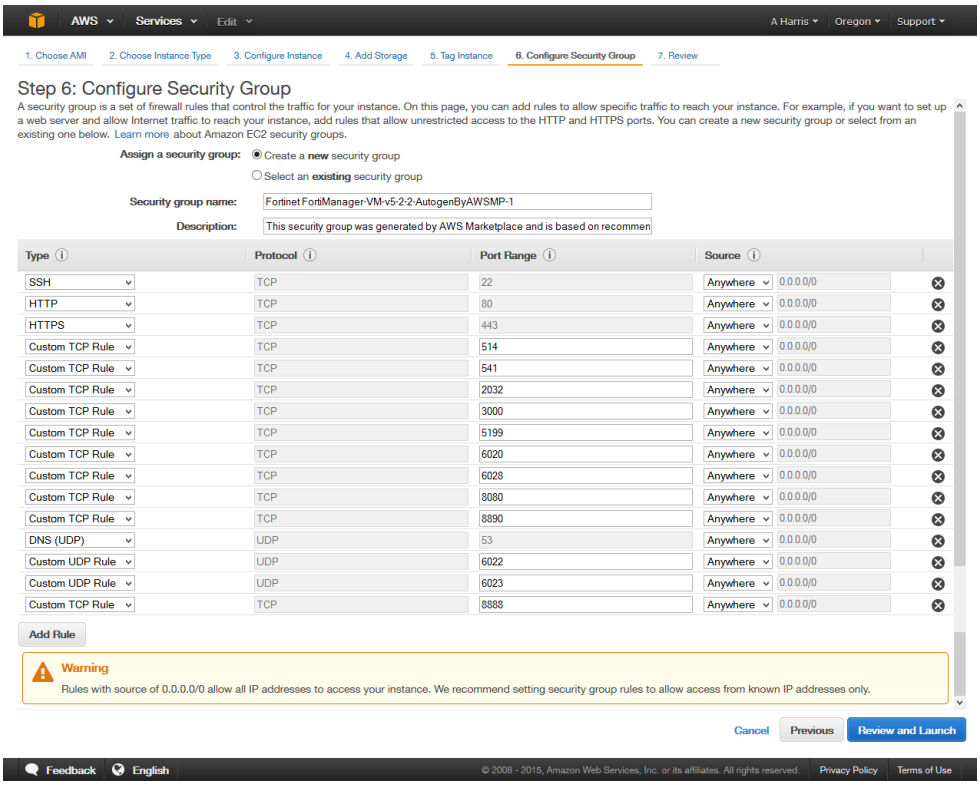
5. Click *Next: Add Storage* to configure the instance's storage based on your requirements.



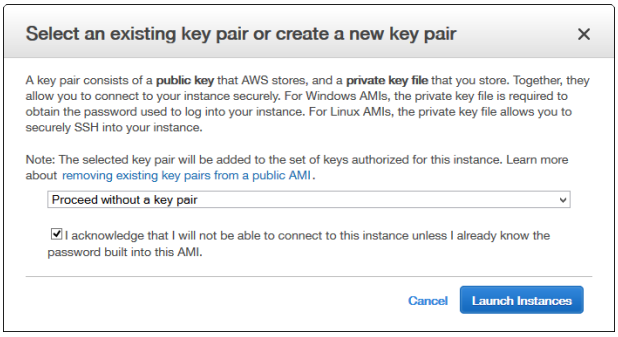
6. Click *Next: Tag Instance* to create a tag. A tag consists of a key-value pair. It is useful to create tags to quickly reference instance items in your deployment. Up to 10 tags can be added.



7. Click *Next: Configure Security Group*, then either create a new security group, or select an existing security group. The default provided security group is based on recommended settings the FortiAnalyzer VM.



8. Click *Review and Launch*. If necessary, decide which boot volume to boot the instance from.
9. Review the instance, including the AMI details, instance type, security groups, instance details, storage, and tags. Edit the configuration as needed.
10. Click *Launch*, select *Proceed without a key pair* from the drop-down list, then select the checkbox acknowledging that you already have the username and password for the AMI.



11. Click *Launch Instances* to launch the new FortiAnalyzer VM instance.
12. To connect to the FortiAnalyzer VM GUI, open a web browser and use the public DNS address as the URL:

    `https://<public DNS address>`
13. Log in with default username `admin` and the instance ID as the password to configure your FortiAnalyzer VM.

In FortiAnalyzer VM 5.4.1 and earlier, if the instance ID is a long ID (19 characters), only the first 10 characters are used as the default password.

Initial Configuration

Before you can connect to the FortiAnalyzer VM you must configure basic configuration via the CLI console. Once configured, you can connect to the FortiAnalyzer VM GUI and upload the FortiAnalyzer VM license file that you downloaded from the Customer Service & Support portal.

The following topics are included in this section:

- GUI access
- Upload the license file
- Configure your FortiAnalyzer VM

GUI access

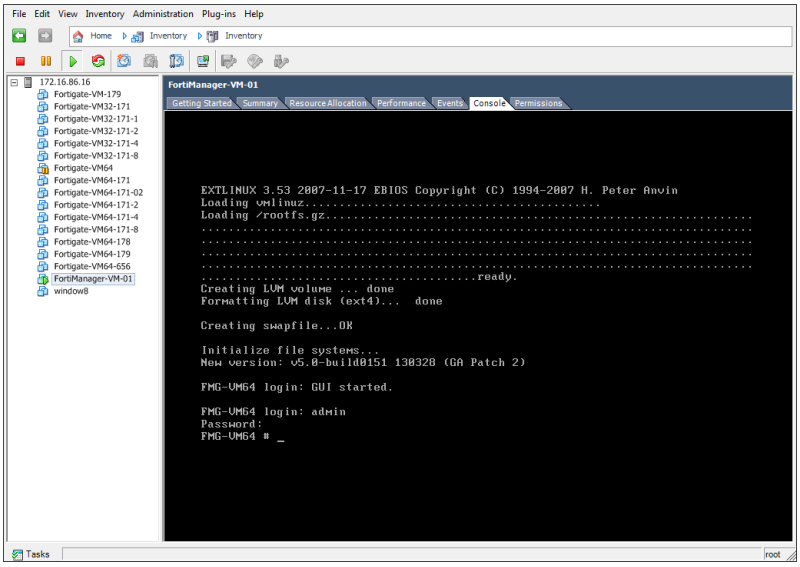
FortiAnalyzer VM AWS and Azure instances do not require any special configuration to enable GUI access. The GUI can be accessed with the public DNS

Enable GUI access

To enable GUI access to the FortiAnalyzer VM you must configure the port1 IP address and network mask of the FortiAnalyzer VM.

To configure the port1 IP address and netmask:

1. In your hypervisor manager, start the FortiAnalyzer VM and access the console window. You might need to press *Enter* to see the login prompt.



2. At the FortiAnalyzer VM login prompt, enter the username *admin*, then press *Enter*. By default, there is no password.
3. Using CLI commands, configure the port1 IP address and netmask.

   For example:

```
config system interface
   edit port1
      set ip <IP address> <Netmask>
end
```

You can also use the *append allowaccess* command to enable other access protocols, such as *auto-ipsec* and *snmp*. The *ping*, *https*, *ssh*, and *fgfm* protocols are enabled by default.
For more information, see the *FortiAnalyzer CLI Reference* in the Fortinet Document Library.

The port management interface should match the first network adapter and virtual switch that you have configured in the hypervisor virtual machine settings.

4. To configure the default gateway, enter the following commands:

```
config system route
   edit 1
      set device port1
      set gateway <gateway_ipv4_address>
end
```

The Customer Service & Support portal does not currently support IPv6 for FortiAnalyzer VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

Connect to the GUI

Once you have configured the port1 IP address and network mask, launch a web browser and enter the IP address you configured for the port management interface. At the login page, enter the user name `admin` and no password, then select *Login*.

The GUI will open with an *Evaluation License* dialog box.

Upload the license file

FortiAnalyzer VM includes a free, full featured 15 day trial.

Before using the FortiAnalyzer VM you must enter the license file that you downloaded from the Customer Service & Support portal upon registration.

To upload the license via the CLI:

1. Open the license file in a text editor and copy the VM license string.
2. In a FortiAnalyzer VM console window, enter the following:

```
execute add-vm-license <"vm license string">
```

See the *FortiAnalyzer CLI Reference*, available from the Fortinet Document Library, for more details on using this command.

To upload the license file via the GUI:

1. In the *Evaluation License* dialog box, select *Enter License*.

   Optionally, you can also select *Upload License* in the *License Information* dashboard widget.
2. In the license upload page, click *Browse*, locate the VM license file (`.lic`) on your computer, then click *OK* to upload the license file.

   A reboot message will be shown, then the FortiAnalyzer VM system will reboot and load the license file.
3. Refresh your browser and log back into the FortiAnalyzer VM with username *admin* and no password.

   The VM registration status appears as valid in the *License Information* widget once the license has been validated.

As a part of the license validation process FortiAnalyzer VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiAnalyzer's IP address has been changed, the FortiAnalyzer VM must be rebooted in order for the system to validate the change and operate with a valid license.

If the IP address in the license file and the IP address configured in the FortiAnalyzer VM do not match, you will receive an error message when you log back into the VM.

If this occurs, you will need to change the IP address in the Customer Service & Support portal to match the management IP and re-download the license file. To change the management IP address, see To edit the FortiAnalyzer VM IP address: on page 10

After an invalid license file has been loaded onto the FortiAnalyzer VM, the GUI will be locked until a valid license file is uploaded. A new license file can be uploaded via the CLI.

Configure your FortiAnalyzer VM

Once the FortiAnalyzer VM license has been validated, you can configure your device. For more information on configuring your FortiAnalyzer VM, see the *FortiAnalyzer Administration Guide* available in the Fortinet Document Library.

Index

FORTINET®

High Performance Network Security